THE INFLUENCERS 2014

GOVINFOSECURITY®

Our spotlight on the most influential people in government information security

GovInfoSecurity presents its ranking of 10 individuals who we see shaping the way that government approaches information security in 2014.

What makes an Influencer? It's a combination of position and know-how. Plus, with the exception of one individual, each of the Influencers has demonstrated the ability to lead and collaborate, characteristics of individuals who have a proven history on getting things done.

For 2014, the No. 1 Influencer we singled out at the time we first published the list was a person yet to be named to a vital government position. That changed on Jan. 30 with President Obama making a key appointment.

10 EDWARD SNOWDEN

At the start of 2013, only his family, friends and colleagues had heard of Snowden. But by year's end, the one-time NSA contractor working as a SharePoint webserver administrator proved to be the most influential person in cybersecurity as the result of his leaking NSA secrets on government surveillance programs. Whether he's a traitor or patriot, the impact of his leaks will sway how the federal government shapes its cybersecurity, privacy and surveillance programs in 2014.

9 ADAM SEDGEWICK

Senior Information Technology Policy Adviser, National Institute of Standards and Technology
In February, the Obama administration will release its cybersecurity framework, a set of voluntary best practices aimed at securing the nation's critical IT infrastructure, and Sedgewick is the government official shepherding the program. Sedgewick will be responsible for getting critical infrastructure operators to adopt the framework, a key goal in securing the infrastructure that Americans depend on.

8 MICHAEL MCCAUL

Chairman, House Homeland Security Committee
As chairman of the House panel with oversight on homeland security, McCaul is the prime sponsor of two cybersecurity bills that have passed the House with bipartisan support that would change the way government approaches IT security. Any compromise between Senate and House versions on cybersecurity reform, including changes to the Federal Information Security Management Act, the law that governs government IT security, must win McCaul's approval.

7 PHYLLIS SCHNECK

Deputy Undersecretary for Cybersecurity, National Protection and Programs Directorate, Department of Homeland Security
On the job as DHS's chief cybersecurity official since September 2013, Schneck offers a different set of experiences than her predecessors. A Ph.D. and patent holder, Schneck's academic and research background reflects out-of-the-box thinking about IT security that should prove useful at DHS expands its influence over securing the nation's critical assets. She champions, for example, developing IT security technology to emulate a human body with a strong immune system to battle infections.

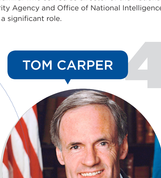
6 MICHAEL DANIEL

Special Assistant to the President, White House Cybersecurity Coordinator
Daniel describes his job as being a "pack herder," getting various stakeholders in and out of government to collaborate on an array of measures to make critical information technologies secure. His primary focus has been on implementing the three objectives of President Obama's February 2013 executive order: cybersthreat information sharing, privacy protection and adoption of IT security best practices.

5 MIKE MCCONNELL

Vice Chairman, Booz Allen Hamilton
A fact of life is that government could not function without employing private contractors. Government contractors hold a lot of sway on how the government addresses cybersecurity, especially those led by individuals who once held high office. Booz Allen furnishes staff and advice to all military branches and the intelligence community. And McConnell, a former vice admiral who served as director of the National Security Agency and Office of National Intelligence, plays a significant role.

4 TOM CARPER



Chairman, Senate Homeland Security and Governmental Affairs Committee
Congress enacted the Federal Information Security Management Act, the law that governs federal government IT security, in 2002, during Carper's first term in the Senate. As Congress' prime champion of FISMA reform, which has stalled in recent years, Carper is now in a position as chairman of the committee with government IT security oversight to get his colleagues to adopt IT security reforms.

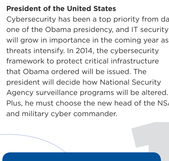
3 JEH JOHNSON

Secretary, Department of Homeland Security
Johnson came to the job in late 2013 with virtually no cybersecurity experience, but the nature of his role makes him an advocate for the administration's cybersecurity policy. The Obama administration has given DHS a lot of sway on getting civilian agencies to improve their IT security as well as working with the private sector on protecting the nation's critical IT assets. Johnson's management skills will be put to the test as DHS builds its depleted IT security workforce.

2 BARACK OBAMA

President of the United States
Cybersecurity has been a top priority from day one of the Obama presidency, and IT security will grow in importance in the coming year as threats intensify. In 2014, the cybersecurity framework to protect critical infrastructure that Obama ordered will be issued. The president will decide how National Security Agency surveillance programs will be altered. Plus, he must choose the new head of the NSA and military cyber commander.

1 MICHAEL ROGERS



Director of the National Security Agency/ Commander, Cyber Command
With Army Gen. Keith Alexander retiring this spring, a new lead was tapped by President Obama to take over the dual-hatted job of the National Security Agency director and military's Cyber Command commander: Navy Vice Adm. Michael Rogers. The combined post will make the veteran cryptographer who has been serving as the head of the Navy Cyber Command the most powerful cybersecurity official in the federal government. In the wake of the Edward Snowden disclosure, Rogers must excel as a skillful politician, effective technocrat and masterful communicator.

2013 Influencers

1. Barack Obama, President of the United States
2. Michael Daniel, Special Assistant to the President and White House Cybersecurity Coordinator
3. Will Pelgrin, CEO, Center for Internet Security, and Founder, Multi-State Information Sharing and Analysis Center
4. Keith Alexander, Director, National Security Agency, and Commander, United States Cyber Command
5. Tom Carper, Chairman, Senate Homeland Security and Governmental Affairs Committee
6. Mark Weatherford, National Protection and Programs Directorate, Deputy Undersecretary for Cybersecurity, Department of Homeland Security
7. Steven VanRoekel, Chief Information Officer, United States Government
8. Michael McCaul, Chairman, House Homeland Security Committee
9. Ron Ross, Fellow and Leader, FISMA Implementation Project, NIST
10. Chris Buse, Chief Information Security Officer, State of Minnesota

ISMG INFORMATION SECURITY MEDIA GROUP

About ISMG
Headquartered in Princeton, New Jersey, Information Security Media Group, Corp. (ISMG) is a media company focusing on Information Technology Risk Management for vertical industries. The company provides news, training, education and other related content for risk management professionals in their respective industries.